

Políticas de Serviços de Hosting Cloud e de Entrega da Oracle

Data Efectiva: Dezembro de 2022; Versão 3.4

ÍNDICE

Índice	2
VISÃO GERAL	4
1 Política de Segurança Cloud Oracle	5
1.1 Práticas de Segurança de Informações da Oracle – Geral	5
1.2 Meios de Salvaguarda de Segurança Física	6
1.3 Controlos de Acesso ao Sistema	6
1.4 Controlos de Acesso a Dados	7
1.5 Encriptação de Utilizador para Ligações Externas	7
1.6 Controlo de Introdução	7
1.7 Separação de Dados e Rede	8
1.8 Confidencialidade e Formação	8
1.9 Gestão de Activos	8
1.10 Políticas Internas de Segurança de Informações da Oracle	8
1.11 Análises e Aplicação da Segurança Interna	8
1.12 Análises Externas	9
1.13 Garantia de Segurança de Software Oracle	9
1.14 Registos de Segurança	9
1.15 Outras Obrigações Relacionadas com a Segurança do Cliente	9
2 Política de Continuidade de Serviços Cloud Oracle	10
2.1 Estratégia de Elevada Disponibilidade de Serviços Cloud Oracle	10
2.2 Estratégia de Cópias de Segurança de Serviços Cloud Oracle	10
2.3 Continuidade Empresarial da Oracle	10
3 Acordo de Nível de Serviço Cloud Oracle	11
3.1 Horário de Funcionamento	11
3.2 Disponibilidade de Serviço	11
3.2.1 Medição de Disponibilidade	11
3.2.2 Relatórios de Disponibilidade	12
3.2.3 Créditos de Serviços	12
3.3 Definição de Tempo de Inactividade Não Planeado	12
3.4 Monitorização	13
3.4.1 Monitorização de Componentes	13
3.4.2 Ferramentas de Teste e Monitorização do Cliente	13
4 Política de Gestão de Alterações Cloud Oracle	13
4.1 Manutenção e Gestão de Alterações Cloud Oracle	13
4.1.1 Manutenção de Segurança Crítica	14
4.1.2 Migrações de Datacenter	14
4.2 Versões de Software	14
4.2.1 Actualizações de Software	14
4.2.2 Fim de Vida	15
5 Política de Suporte Cloud Oracle	15

5.1	Termos do Suporte Cloud Oracle	15
5.1.1	Valores de Suporte	15
5.1.2	Período de Suporte	15
5.1.3	Contactos Técnicos	15
5.1.4	Suporte Cloud Oracle	16
5.2	Sistemas de Suporte a Clientes Cloud Oracle	16
5.2.1	Portal de Suporte a Clientes Oracle Cloud	16
5.2.2	Suporte por Telefone em Tempo Real	16
5.3	Definições de Severidade	17
5.3.1	Severidade 1	17
5.3.2	Severidade 2	17
5.3.3	Severidade 3	17
5.3.4	Severidade 4	17
5.4	Alteração do Nível de Severidade de Requisições de Serviços	18
5.4.1	Nível de Severidade Inicial	18
5.4.2	Redução do Nível de Requisições de Serviços	18
5.4.3	Aumento do Nível de Requisições de Serviços	18
5.4.4	Conformidade com as Definições de Nível de Severidade	18
5.5	Escalonamento de Requisições de Serviços	18
6	Política de Resolução e Suspensão Cloud Oracle	19
6.1	Resolução de Serviços Cloud Oracle	19
6.2	Resolução de Serviços de Testes Piloto	19
7	UTILIZAÇÃO DOS SERVIÇOS	20

VISÃO GERAL

As presentes Políticas de Serviços de Hosting Cloud e de Entrega da Oracle ("Políticas de Entrega") descrevem os Serviços Cloud Oracle encomendados pelo Cliente. Estas Políticas de Entrega podem referir outros documentos relacionados com a Política de Serviços Cloud Oracle; qualquer referência a "Cliente" nas presentes Políticas de Entrega ou nesses outros documentos relativos à Política será considerada como uma referência ao "Cliente" conforme definido na Nota de Encomenda do Cliente.

Quaisquer referências a "Região do Datacenter" de um Serviço Cloud nas presentes Políticas de Entrega refere-se à região geográfica listada na Nota de Encomenda do Cliente para tais Serviços ou, se aplicável, à região geográfica que o Cliente seleccionou ao activar a instância do produto para tais Serviços. Para efeitos da Região do Datacenter aplicável aos Serviços Cloud encomendados do Cliente, aplica-se o seguinte:

- "Europa" refere-se aos países membros da União Europeia, Reino Unido e Suíça, colectivamente; e
- "APAC" refere-se à região geografia da Ásia-Pacífico, com excepção da China, dado que a Oracle não tem Datacenters na China.

No que diz respeito aos Serviços Cloud Oracle encomendados pelo Cliente, os Conteúdos do Cliente serão armazenados na Região do Datacenter aplicável a esses Serviços. A Oracle pode replicar os Conteúdos do Cliente noutras localizações na Região do Datacenter identificada como suporte à redundância de dados. Os termos iniciados com letra maiúscula que não são de outra forma definidos nas presentes Políticas de Entrega terão o significado atribuído no Acordo Oracle, Nota de Encomenda do Cliente ou política, conforme aplicável. As presentes Políticas de Entrega são actualizadas duas vezes por ano.

A Nota de Encomenda do Cliente ou as Especificações de Serviço da Oracle (conforme definido no Acordo do Cliente para Serviços Cloud Oracle, que inclui documentação Pilar de Serviços Cloud Oracle, Descrições de Serviço e definições adicionais fornecidas no Acordo de Serviços Cloud Oracle) pode incluir detalhes adicionais ou excepções relacionados com Serviços Cloud Oracle específicos. A documentação Pilar de Serviços Cloud Oracle, as Descrições de Serviços e a Documentação do Programa para os Serviços Cloud Oracle estão disponíveis em www.oracle.com/contracts.

Os Serviços Cloud Oracle são fornecidos ao abrigo dos termos do Acordo da Oracle, da Nota de Encomenda do Cliente e das Especificações de Serviço aplicáveis a esses Serviços. A prestação dos Serviços Cloud Oracle por parte da Oracle está dependente do cumprimento por parte do Cliente e dos Utilizadores do Cliente das obrigações e responsabilidades definidas nesses documentos e nas políticas incorporadas. As presentes Políticas de Entrega e os documentos mencionados no presente documento estão sujeitos a alterações a critério da Oracle; todavia, as alterações às Políticas da Oracle não resultarão numa redução material do nível de desempenho, funcionalidade, segurança ou disponibilidade dos Serviços Cloud Oracle fornecidos durante o Período de Serviços da Nota de Encomenda do Cliente.

Os Serviços Cloud Oracle são implementados em datacenters ou prestadores de serviços de infra-estruturas externos contratados pela Oracle, excepto no caso dos Serviços Cloud Oracle at Customer. Os Serviços Cloud Oracle at Customer são Serviços Cloud Públicos que são implementados no

datacenter do Cliente ou num datacenter de terceiros contratado pelo Cliente. O Cliente pode adquirir estes Serviços na sua forma autónoma ou estes podem ser implementados como plataforma subjacente de outros Serviços Cloud Oracle. No que diz respeito a Serviços Cloud Oracle at Customer, a Oracle fornecerá ao datacenter do Cliente determinados componentes de hardware, incluindo equipamento de gateway, necessários para a Oracle prestar estes Serviços. O Cliente é responsável por fornecer sistemas de refrigeração, fontes de alimentação e espaço adequados para implementar o hardware Oracle (incluindo equipamento de gateway) e por garantir uma conectividade de rede adequada para que a equipa de Operações Cloud Oracle aceda aos serviços. A Oracle é a única responsável pela manutenção dos componentes de hardware da Oracle (incluindo equipamento de gateway).

As presentes Políticas de Entrega não se aplicam a Oracle BigMachines Express, Oracle ETAWorkforce ou quaisquer outras ofertas Cloud Oracle, conforme especificado pela Oracle na Nota de Encomenda do Cliente ou nas Descrições de Serviço aplicáveis.

1 POLÍTICA DE SEGURANÇA CLOUD ORACLE

1.1 Práticas de Segurança de Informações da Oracle – Geral

A Oracle adoptou práticas e controlos de segurança para os Serviços Cloud Oracle que foram concebidos para proteger a confidencialidade, integridade e disponibilidade dos Conteúdos do Cliente alojados pela Oracle nos Serviços Cloud Oracle do Cliente e para proteger os Conteúdos do Cliente de quaisquer actividades de tratamento não autorizadas, tais como perda ou destruição ilegal de dados. A Oracle trabalha continuamente no sentido de reforçar e melhorar estas práticas e controlos de segurança.

Os Serviços Cloud Oracle funcionam ao abrigo de práticas em conformidade com o Código de Práticas ISO/IEC 27002 relativo a controlos de segurança de informações, a partir do qual é seleccionado um conjunto abrangente de controlos. Os Serviços Cloud Oracle estão alinhados com as publicações do National Institute of Standards and Technology (Instituto nacional norte-americano de normas e tecnologia) ("NIST") 800-53 e 800-171.

As práticas de segurança de informações Cloud da Oracle estabelecem e regem áreas de segurança aplicáveis aos Serviços Cloud Oracle e à utilização por parte do Cliente desses Serviços Cloud Oracle. O pessoal da Oracle (incluindo colaboradores, contratados e colaboradores temporários) está sujeito às práticas de segurança de informações da Oracle e a quaisquer políticas adicionais que regulamentem o seu emprego ou os serviços prestados à Oracle.

A Oracle adopta uma abordagem holística em relação à segurança de informações, implementando uma estratégia de segurança e defesa multifacetada, na qual a rede, sistema operativo, base de dados e procedimentos e práticas de segurança de software se complementam entre si com uma supervisão, administração e controlos internos reforçados.

No que diz respeito aos Serviços Cloud Oracle que permitem ao Cliente configurar a respectiva postura de segurança, salvo disposição em contrário, o Cliente é responsável por configurar, operar, manter e proteger os sistemas operativos e outro software associado destes Serviços Cloud Oracle

seleccionados (incluindo os Conteúdos do Cliente) que não são fornecidos pela Oracle. O Cliente é responsável por manter a segurança, a protecção e cópias de segurança adequadas dos Conteúdos do Cliente, o que pode incluir a utilização de tecnologia de encriptação para proteger os Conteúdos do Cliente contra acesso não autorizado e arquivo de rotina.

1.2 Meios de Salvaguarda de Segurança Física

A Oracle emprega medidas concebidas para evitar o acesso não autorizado de pessoas a instalações informáticas que alojam os Conteúdos do Cliente, como o recurso a pessoal de segurança, edifícios seguros e instalações de datacenter designadas. A Oracle fornece instalações informáticas seguras tanto para escritórios como para infra-estruturas de produção cloud. Actualmente, os controlos comuns entre escritórios e co-localizações/datacenters controlados pela Oracle incluem, por exemplo, o seguinte:

- O acesso físico requer autorização e é monitorizado
- Todos os colaboradores e visitantes têm de apresentar uma identificação oficial visível enquanto estiverem no local
- Os visitantes têm de assinar um registo de visitantes e ser acompanhados e/ou monitorizados enquanto estiverem no local
- A posse de chaves/cartões de acesso e a capacidade de aceder aos vários locais são monitorizadas. Os colaboradores que deixem de trabalhar na Oracle têm de devolver as chaves/cartões

Há meios de salvaguarda de segurança física adicionais para os datacenters Cloud controlados pela Oracle, sendo incluídos actualmente meios de salvaguarda como os que se seguem:

- As instalações são monitorizadas por um circuito fechado de televisão (CFTV)
- As entradas são protegidas por barreiras físicas concebidas para evitar a entrada não autorizada de veículos
- As entradas são vigiadas 24 horas por dia, 365 dias por ano, por seguranças que procedem ao reconhecimento visual de identificação e à gestão do acompanhamento de visitantes
- Meios de salvaguarda relacionados com perigos ambientais
- Qualquer movimentação física de equipamento é controlada por recepção em mão e outros procedimentos de controlo de alterações autorizados
- Os cabos de rede estão protegidos por condutas e, quando possível, evitam percursos através de áreas públicas

A presente secção não é aplicável a Serviços Oracle Cloud at Customer. O Cliente tem de fornecer as suas próprias instalações informáticas seguras para o hosting e funcionamento de hardware relacionado com os Serviços Oracle Cloud at Customer (incluindo o equipamento de gateway) e ligações de rede necessário para a Oracle prestar os Serviços Oracle Cloud at Customer.

1.3 Controlos de Acesso ao Sistema

As políticas da Oracle exigem que sejam aplicados os seguintes controlos: autenticação através de palavras-passe e/ou autenticação multifactor, controlos de autorização documentados e registo de

acesso. Todo o acesso remoto à Rede Cloud Oracle pela equipa da Oracle com acesso aos Conteúdos do Cliente é restringido através da utilização de uma Virtual Private Network, que utiliza autenticação multifactor. Para além da utilização requerida de uma Virtual Private Network, antes de a equipa da Oracle ser autorizada a aceder à Rede Cloud Oracle, a Oracle realiza verificações de postura de dispositivos e tem controlos em vigor, como anfitriões de bastião. A Oracle proíbe (através de políticas e de controlos técnicos) a utilização de dispositivos pessoais para aceder à Rede Cloud Oracle e aos Serviços Cloud Oracle.

Para Serviços Cloud alojados na Oracle: (i) os inícios de sessão em ambientes de Serviços Cloud são registados; e (ii) o acesso lógico aos datacenters é restrito e protegido.

1.4 Controlos de Acesso a Dados

Para componentes de serviço geridos pela Oracle, o acesso da Oracle aos Conteúdos do Cliente está limitado ao pessoal autorizado.

No que se refere ao acesso dos Serviços Cloud Oracle por parte da equipa da Oracle (incluindo os Conteúdos do Cliente existentes nos Serviços Cloud Oracle), a Oracle exerce os controlos de acesso baseados em funções (Role Based Access Controls (RBAC), doravante "RBAC") e recorre aos princípios de gestão de acesso de "necessidade de conhecimento", "privilégios mínimos" e "separação de tarefas". Além disso, a Oracle fornece um mecanismo que permite ao Cliente controlar o acesso dos respectivos Utilizadores aos Serviços Cloud Oracle e aos Conteúdos do Cliente.

1.5 Encriptação de Utilizador para Ligações Externas

O acesso do Cliente aos Serviços Cloud Oracle é realizado através de um protocolo de comunicação seguro fornecido pela Oracle. Se o acesso for realizado através de uma ligação Transport Layer Security (TLS), essa ligação é negociada para uma encriptação de, pelo menos, 128 bits. A chave privada utilizada para gerar a chave de cifra tem, no mínimo, 2048 bits. O TLS é implementado ou configurável em todas as aplicações com certificação TLS baseadas na Web e implementadas na Oracle. Recomenda-se a utilização dos browsers mais recentes que se encontrem disponíveis e certificados para programas Oracle, compatíveis com forças de codificação superiores e com uma segurança melhorada, para estabelecer ligações a programas com ligação à Web. A lista de browsers certificados para cada versão de Serviços Cloud Oracle será disponibilizada através de um portal acessível ao Cliente ou na Descrição dos Serviços correspondente para os Serviços Cloud Oracle. Em alguns casos, um Web site de terceiros que o Cliente pretenda integrar com os Serviços Cloud Oracle, como um serviço de redes sociais, pode não aceitar uma ligação encriptada. Nos Serviços Cloud Oracle em que sejam permitidas pela Oracle ligações HTTP com o Web site de terceiros, a Oracle activará essas ligações HTTP além da ligação HTTPS.

1.6 Controlo de Introdução

A origem dos Conteúdos do Cliente está sob o controlo e a responsabilidade do Cliente e a integração dos Conteúdos do Cliente nos Serviços Cloud Oracle é gerida pelo Cliente.

1.7 Separação de Dados e Rede

Os Conteúdos do Cliente estão separados de forma lógica ou física dos conteúdos de outros clientes alojados nos Serviços Cloud Oracle. Todas as redes Oracle Public Cloud são separadas das Redes empresariais da Oracle.

1.8 Confidencialidade e Formação

A equipa da Oracle que pode ter acesso aos Conteúdos do Cliente está sujeita a acordos de confidencialidade. Todas as equipas da Oracle que têm acesso aos Conteúdos do Cliente têm de frequentar formação de sensibilização sobre protecção de informações após contratação. Posteriormente, todas as equipas da Oracle que têm acesso aos Conteúdos do Cliente têm de frequentar formação de acordo com a documentação de formação de sensibilização sobre segurança e privacidade da Oracle relevante.

1.9 Gestão de Activos

A Oracle é responsável pela protecção e pelo inventário dos activos dos Serviços Cloud Oracle. As responsabilidades podem incluir a análise e a autorização de pedidos de acesso a pessoas com uma necessidade empresarial e a manutenção de um inventário de activos.

O Cliente é responsável pelos activos que controla e que utilizam ou integram os Serviços Cloud Oracle, incluindo: a classificação de informação adequada aos Conteúdos do Cliente e se os controlos documentados fornecidos pelos Serviços Cloud Oracle são adequados aos Conteúdos do Cliente. O Cliente tem de possuir ou obter todas as autorizações e outros fundamentos jurídicos referentes à recolha e utilização das informações fornecidas pelos titulares de dados, incluindo as autorizações e outros fundamentos jurídicos necessários para prestar os Serviços Cloud Oracle.

1.10 Políticas Internas de Segurança de Informações da Oracle

As políticas de segurança de informações Cloud da Oracle estabelecem e regem áreas de segurança aplicáveis aos Serviços Cloud Oracle e à utilização por parte do Cliente dos Serviços Cloud Oracle. O pessoal da Oracle está sujeito às Políticas de Segurança de Informações Empresariais da Oracle e a quaisquer políticas adicionais que regulamentem o seu emprego ou os serviços prestados à Oracle. O Information Security Program ("ISP") da Oracle consiste em políticas documentadas que consideram factores de risco, incluindo factores digitais e de segurança, com procedimentos, normas e directrizes derivados necessários para a operacionalização eficaz de políticas. O ISP da Oracle foi concebido para garantir confidencialidade, integridade, privacidade, continuidade e disponibilidade dos Conteúdos do Cliente alojados pela Oracle nos Serviços Cloud Oracle do Cliente através de controlos e práticas de gestão de segurança eficazes. O ISP da Oracle é analisado anualmente pela Comissão de Supervisão de Segurança da Oracle e actualizado conforme necessário.

1.11 Análises e Aplicação da Segurança Interna

A Oracle utiliza regularmente processos internos para testar, aferir, avaliar e manter a eficácia das medidas de segurança técnica e organizacional descritas nesta secção.

1.12 Análises Externas

A Oracle pode realizar análises independentes dos Serviços Cloud Oracle, recorrendo a terceiros, nas seguintes áreas (o âmbito destas análises pode variar consoante o Serviço e o país):

- SOC 1 (baseados nas normas Statement on Standards for Attestation Engagements (SSAE) N.º 18) e/ou SOC 2
- Outros testes de segurança de terceiros independentes para analisarem a eficácia dos controlos técnicos e administrativos

As informações relevantes destas análises podem ser disponibilizadas aos clientes.

1.13 Garantia de Segurança de Software Oracle

A Garantia de Segurança de Software Oracle (Oracle Software Security Assurance, doravante "OSSA") constitui a metodologia da Oracle para incorporar segurança na concepção, construção, teste e manutenção dos respectivos Serviços e produtos, incluindo os Serviços Cloud Oracle. O programa OSSA encontra-se descrito em <https://www.oracle.com/corporate/security-practices/assurance/>.

1.14 Registos de Segurança

Os registos são gerados para actividades relevantes para a segurança em sistemas operativos. Os sistemas são configurados para registar actividades de segurança predefinidas, acesso a informações ou programas, eventos do sistema, como alertas, mensagens de consola e erros do sistema. A Oracle analisa os registos quanto a incidentes e para efeitos forenses; as anomalias identificadas são integradas no processo de gestão de incidentes. Os registos de segurança são armazenados no sistema de Gestão de Eventos e Informações de Segurança (ou num sistema equivalente) num formato nativo e inalterado e detidos de acordo com as políticas internas da Oracle. Tais registos são detidos online durante um mínimo de um (1) ano. Estes registos são detidos e utilizados pela Oracle para as respectivas operações de segurança interna dos Serviços Cloud Oracle.

1.15 Outras Obrigações Relacionadas com a Segurança do Cliente

O Cliente é responsável por:

- Implementar o seu próprio sistema completo de procedimentos, standards e políticas operacionais e de segurança, de acordo com os requisitos empresariais e avaliações de risco do Cliente
- Garantir que os dispositivos de utilizador final cumprem os requisitos de browser da Web e os requisitos mínimos de largura de banda da rede para aceder aos Serviços Cloud Oracle
- Gerir os controlos de segurança dos dispositivos de clientes para que as verificações de malware e antivírus sejam efectuadas em dados ou ficheiros antes da importação ou carregamento de dados para os Serviços Cloud Oracle
- Manter as contas geridas pelo Cliente em conformidade com as melhores práticas de segurança e políticas do Cliente
- Adicionalmente, no que diz respeito a Serviços Cloud Oracle at Customer, o Cliente é responsável pelo seguinte:

- Segurança física e de rede adequada;
- Monitorização da segurança para reduzir o risco de ameaças em tempo real e impedir o acesso não autorizado aos Serviços Cloud Oracle do Cliente a partir das respectivas redes; isto inclui sistemas de detecção de intrusão, controlos de acesso, firewalls e qualquer outra monitorização de rede e quaisquer ferramentas de gestão geridas pelo Cliente.

2 POLÍTICA DE CONTINUIDADE DE SERVIÇOS CLOUD ORACLE

2.1 Estratégia de Elevada Disponibilidade de Serviços Cloud Oracle

A Oracle implementa os Serviços Cloud Oracle numa infra-estrutura informática resiliente concebida para manter a disponibilidade e a continuidade de serviço caso ocorra um incidente que afecte os Serviços. Os datacenters mantidos pela Oracle para alojar os Serviços Cloud Oracle dispõem de redundância de componentes e fontes de alimentação com geradores de reserva, sendo que a Oracle pode incorporar redundância numa ou mais camadas, incluindo a infra-estrutura de rede, servidores de programas, servidores de bases de dados e/ou armazenamento.

2.2 Estratégia de Cópias de Segurança de Serviços Cloud Oracle

A Oracle efectua periodicamente cópias de segurança dos Conteúdos do Cliente na instância de produção do Cliente dos Serviços Cloud Oracle para utilização exclusiva da Oracle, no sentido de minimizar a perda de dados na eventualidade de ocorrer algum incidente. As cópias de segurança são armazenadas no local principal utilizado para prestar os Serviços Cloud Oracle, bem como em localizações alternativas para efeitos de retenção. Uma cópia de segurança de produção é tipicamente mantida online ou offline durante um período de, pelo menos, sessenta (60) dias após a data em que a cópia de segurança é efectuada. Normalmente, a Oracle não actualiza, insere, elimina ou restaura dados do Cliente em nome deste. Contudo, a título excepcional e sujeito a aprovação por escrito, a Oracle pode auxiliar o Cliente no restauro de dados que o Cliente possa ter perdido como resultado das suas próprias acções.

No que diz respeito a Serviços Cloud Oracle que permitem ao Cliente configurar cópias de segurança de acordo com as próprias políticas, o Cliente é responsável por realizar cópias de segurança e restauros do Conteúdo do Cliente. Além disso, recomenda-se que o Cliente desenvolva um plano de continuidade empresarial para garantir a continuidade das próprias operações em caso de desastre.

2.3 Continuidade Empresarial da Oracle

Durante a vigência, a Oracle manterá sempre um plano pertencente às operações internas da Oracle com o objectivo de minimizar qualquer interrupção relacionada com a prestação dos serviços em caso de ocorrência de desastres, perturbações ou eventos de força maior ("Plano BC").

O Plano BC estabelece, documenta e implementa processos, procedimentos e controlos para garantir que as disposições de segurança aplicáveis aos Serviços Cloud Oracle não são reduzidas caso o Plano BC seja invocado. O objectivo do Plano BC é fornecer, entre outros aspectos, resiliência às operações

internas da Oracle para assegurar a continuidade e manutenção dos Serviços Cloud Oracle, independentemente da causa.

3 ACORDO DE NÍVEL DE SERVIÇO CLOUD ORACLE

3.1 Horário de Funcionamento

Os Serviços Cloud Oracle são concebidos para estarem disponíveis 24 horas por dia, 7 dias por semana, 365 dias por ano, excepto durante períodos de manutenção, actualizações de tecnologia e conforme estabelecido de outra forma no Acordo Oracle, na Nota de Encomenda do Cliente e no presente *Acordo de Nível de Serviço Cloud Oracle*.

3.2 Disponibilidade de Serviço

Após a activação por parte da Oracle do Serviço Cloud Oracle de produção do Cliente, a Oracle trabalha no sentido de cumprir a Meta de Nível de Disponibilidade de Serviço, ou Meta de Tempo de Actividade do Serviço, de 99,9%. Isto conforme os termos estabelecidos na documentação Pillar relativa a Serviços Cloud Oracle para o Serviço Cloud Oracle aplicável (ou qualquer outra Meta de Nível de Disponibilidade de Serviço ou Meta de Tempo de Actividade do Serviço especificada pela Oracle para o Serviço Cloud Oracle aplicável presente nessa documentação).

O disposto acima está dependente da conformidade por parte do Cliente com os requisitos mínimos de configuração técnica recomendados pela Oracle para aceder e utilizar os Serviços Cloud Oracle a partir da infra-estrutura de rede do Cliente e das estações de trabalho de utilizador do Cliente, conforme estipulado na Documentação do Programa relativa a Serviços Cloud Oracle aplicáveis.

3.2.1 Medição de Disponibilidade

Após o fim de cada mês de calendário do Período de Serviços aplicável, a Oracle mede o Nível de Disponibilidade do Serviço ou o Tempo de Actividade do Serviço ao longo do mês imediatamente anterior, dividindo a diferença entre o número total de minutos no período de medição mensal e qualquer Tempo de Inactividade Não Planeado (conforme definido abaixo) pelo número total de minutos no período de medição e multiplicando o resultado por 100, de modo a obter um valor percentual.

$$\left(\frac{\text{Número de minutos no mês} - \text{Número de minutos de tempo de inactividade não planeado}}{\text{Número de minutos no mês}} \right) * 100$$

Número de minutos num mês de trinta (30) dias = 30 dias * 24 horas por dia * 60 minutos por hora

Número de minutos não planeados no mês = minutos de tempo de inactividade não planeado definidos na Secção 3.3 (Definição de Tempo de Inactividade Não Planeado) abaixo.

Exemplo: Junho tem 30 dias = 30 * 24 * 60 = 43.200 minutos no mês

Em caso de ocorrência de noventa (90) minutos de tempo de inactividade não planeado no mês de Junho, a equação seria:

$$((43.200 - 90) / 43.200) * 100 = 99,8\% \text{ de Nível de Disponibilidade de Serviço}$$

3.2.2 Relatórios de Disponibilidade

A Oracle fornecerá ao Cliente acesso a um portal de notificações para clientes. Este portal fornecerá métricas sobre o Nível de Disponibilidade do Serviço dos Serviços Cloud Oracle que o Cliente adquiriu ao abrigo da respectiva Nota de Encomenda. No que diz respeito aos Serviços Cloud Oracle cujas métricas não estão disponíveis através do portal de notificações para clientes, a Oracle fornecerá métricas sobre o Nível de Disponibilidade do Serviço mediante a recepção de uma Requisição de Serviços apresentada pelo Cliente à Oracle que solicite as métricas.

3.2.3 Créditos de Serviços

O Cliente pode receber Créditos de Serviços caso o Nível Previsto de Disponibilidade do Serviço ou Tempo de Actividade Previsto do Serviço para os Serviços Cloud Oracle, adquiridos pelo Cliente ao abrigo da respectiva Nota de Encomenda, sejam inferiores ao Nível Previsto de Disponibilidade do Serviço ou Tempo de Actividade Previsto do Serviço definidos e aplicáveis para tais Serviços. Os Créditos de Serviços são definidos na documentação Pilar relativa a Serviços Cloud Oracle ou nas Descrições dos Serviços aplicáveis aos Serviços Cloud Oracle adquiridos pelo Cliente. Não obstante as disposições na presente secção, se a Nota de Encomenda do Cliente com a Oracle ou as Especificações de Serviço aplicáveis à Nota de Encomenda do Cliente para um determinado Serviço Cloud Oracle fornecer um direito para receber um valor mais elevado dos Créditos de Serviços, o Cliente pode receber os Créditos de Serviços ao abrigo da disposição que fornece o valor mais elevado de Créditos de Serviços aos Cliente, mas o Cliente não pode recuperar os Créditos de Serviços ao abrigo de múltiplas disposições para o mesmo caso.

3.3 Definição de Tempo de Inatividade Não Planeado

Os Serviços Cloud Oracle são implementados em instalações informáticas resilientes com infra-estruturas resilientes, ligações de rede redundantes e fontes de alimentação em cada instalação de hosting.

"Tempo de Inatividade Não Planeado" significa qualquer período durante o qual um problema com os Serviços Cloud Oracle impede a conectividade do Cliente. O Tempo de Inatividade Não Planeado não inclui quaisquer períodos durante os quais os Serviços Cloud Oracle ou quaisquer componentes de Serviços Cloud Oracle não estão disponíveis devido a: (i) manutenções programadas; (ii) circunstâncias fora do controlo da Oracle e outros eventos de força maior (por exemplo, interrupções iniciadas a pedido do Cliente, interrupções provocadas por infra-estruturas, como equipamento eléctrico, de telecomunicações, rede ou outro equipamento de conectividade não-Oracle, ataques de segurança, desastres naturais ou eventos políticos); (iii) quaisquer acções ou falta de acções por parte do Cliente, dos Utilizadores do Cliente ou de terceiros (além de agentes Oracle ou outros que a Oracle tenha contratado para prestar os Serviços Cloud Oracle); ou (iv) qualquer suspensão pela Oracle, autorizada ao abrigo do Acordo Oracle do Cliente ou Nota de Encomenda do Cliente. Além disso, relativamente aos Serviços Cloud Oracle at Customer, Tempo de Inatividade Não Planeado também não inclui tempo de inatividade nem indisponibilidade: (i) do datacenter do Cliente (por exemplo, devido a manutenção); ou (ii) que ocorra fora do horário no local (onsite) estipulado na Nota de Encomenda do Cliente relativa ao pessoal da equipa de Operações Cloud Oracle no datacenter do Cliente.

3.4 Monitorização

A Oracle utiliza uma variedade de ferramentas de software para monitorizar a disponibilidade e desempenho dos Serviços Cloud Oracle e o funcionamento dos componentes de rede e infra-estrutura. A Oracle não monitoriza nem resolve desvios sofridos por quaisquer componentes que não sejam geridos pela Oracle utilizados pelo Cliente nos Serviços Cloud Oracle, tais como aplicações que não sejam da Oracle.

3.4.1 Monitorização de Componentes

A Oracle monitoriza o hardware que suporta os Serviços Cloud Oracle e, actualmente, gera alertas para componentes de rede monitorizados, tais como CPU, memória, armazenamento, base de dados e outros componentes. A equipa de Operações Cloud Oracle monitoriza alertas associados a desvios em relação aos limiares definidos pela Oracle e acompanha os procedimentos operacionais standard para investigar e resolver problemas subjacentes.

3.4.2 Ferramentas de Teste e Monitorização do Cliente

A Oracle permite que o Cliente conduza testes funcionais limitados para os Serviços Cloud Oracle na instância de teste do Cliente. As regras específicas para testes podem ser encontradas na Documentação do Programa.

A Oracle fornece regularmente testes de penetração e de vulnerabilidade e avaliações de segurança à infra-estrutura, plataformas e aplicações da Cloud Oracle para validar e melhorar a segurança geral dos Serviços Cloud Oracle. A documentação do Programa de Serviços Cloud Oracle descreve quando e como o Cliente pode avaliar ou testar quaisquer componentes geridos ou criados através dos Serviços Cloud Oracle, incluindo aplicações, bases de dados, outro software aplicável não-Oracle, código ou a utilização de ferramentas de fragmentação de dados.

A Oracle reserva-se o direito de remover ou desactivar o acesso a quaisquer ferramentas ou tecnologias que infrinjam as directrizes referidas na presente secção ou na documentação do Programa de Serviços Cloud Oracle aplicável, sem qualquer responsabilidade perante o Cliente.

4 POLÍTICA DE GESTÃO DE ALTERAÇÕES CLOUD ORACLE

4.1 Manutenção e Gestão de Alterações Cloud Oracle

A equipa de Operações Cloud Oracle efectua alterações à infra-estrutura de hardware cloud, software operativo, software de produtos e software de aplicações de suporte fornecido pela Oracle como parte dos Serviços Cloud Oracle para manter a estabilidade operacional, a disponibilidade, a segurança, o desempenho e a actualização dos Serviços Cloud Oracle. A Oracle segue procedimentos de gestão de alterações formais de modo a fornecer a análise, teste e aprovação necessários às alterações, antes da aplicação no Serviço de produção.

As alterações feitas através de procedimentos de gestão de alterações incluem actividades de manutenção de serviço e sistema, actualizações e alterações específicas do Cliente. Os procedimentos de gestão de alterações aos Serviços Cloud Oracle são concebidos para minimizar a interrupção do Serviço durante a implementação de alterações.

A Oracle reserva períodos de manutenção específicos para alterações que possam exigir a indisponibilidade dos Serviços Cloud Oracle durante o período de manutenção. A Oracle trabalha no sentido de garantir que os procedimentos de gestão de alterações são realizados durante janelas de manutenção programadas, tendo em consideração períodos de tráfego reduzido e requisitos geográficos.

A Oracle fornecerá uma notificação prévia relativa a alterações ao calendário de períodos de manutenção standard. Para actualizações e alterações específicas do Cliente, sempre que possível, a Oracle coordenará os períodos de manutenção com o Cliente.

Para alterações em que esteja prevista a interrupção do Serviço, a duração dos períodos de manutenção planeada não está incluída nos cálculos de minutos de Tempo de Inactividade Não Planeado no período de medição mensal para o Nível de Disponibilidade de Serviço (consulte o *Acordo de Nível de Serviço Cloud Oracle* acima). A Oracle envida esforços comercialmente razoáveis para minimizar a utilização destes períodos de manutenção programados e a duração de eventos de manutenção que provoquem interrupções no Serviço.

No que diz respeito a Serviços Cloud Oracle que permitam ao Cliente realizar actividades de manutenção, o Cliente é responsável por configurar e manter os sistemas operativos e outro software associado.

4.1.1 Manutenção de Segurança Crítica

Pode ser solicitado à Oracle que execute manutenção de segurança crítica para proteger a segurança dos Serviços Cloud Oracle. A manutenção de segurança crítica é necessária para resolver uma situação exigente (por exemplo: vulnerabilidade de segurança) no Serviço Cloud Oracle ou infraestrutura Oracle que apenas possa ser tratada em caso de emergência. A Oracle trabalha no sentido de minimizar o recurso a manutenção de segurança crítica e, conforme seja considerado razoável, trabalhará para fornecer um aviso prévio com vinte e quatro (24) horas de antecedência para qualquer operação de manutenção de segurança crítica que exija uma interrupção de serviço fora de períodos de manutenção programados.

4.1.2 Migrações de Datacenter

A Oracle pode migrar os Serviços Cloud Oracle do Cliente implementados em datacenters mantidos pela Oracle entre datacenters de produção dentro da mesma Região do Datacenter, conforme considerado necessário pela Oracle ou em caso de "Disaster Recovery" (Recuperação de Desastres). Para as migrações de datacenter com fins que não de "Disaster Recovery" (Recuperação de Desastres), a Oracle fornecerá ao Cliente uma notificação com, no mínimo, trinta (30) dias de antecedência.

4.2 Versões de Software

4.2.1 Actualizações de Software

A Oracle requer que todos os Clientes de Serviços Cloud Oracle mantenham as versões de software dos Serviços Cloud Oracle actualizadas em relação às versões de software que a Oracle designa como Disponíveis de Forma Geral para esses Serviços Cloud Oracle. Após o lançamento de cada versão

disponível de forma geral, serão lançadas actualizações de software necessárias para manter as versões actualizadas desses Serviços Cloud Oracle. As obrigações da Oracle ao abrigo das presentes Políticas de Entrega (incluindo a *Política de Continuidade de Serviços Cloud Oracle*, o *Acordo de Nível de Serviço Cloud Oracle* e a *Política de Suporte Cloud Oracle*) dependem da manutenção pelo Cliente da versão disponível de forma geral mais actualizada. A Oracle não é responsável por problemas de desempenho, funcionalidade, disponibilidade ou segurança detectados nos Serviços Cloud Oracle que possam resultar da execução de versões anteriores.

4.2.2 Fim de Vida

A Oracle alojará e fornecerá suporte apenas às versões disponíveis de forma geral para um Serviço Cloud Oracle. Todas as outras versões do Serviço Cloud Oracle são consideradas como estando em "Fim de Vida". O Cliente tem de completar a actualização dos Serviços Cloud Oracle para a versão mais recente antes do Fim de Vida de uma determinada versão. O Cliente confirma que a não actualização antes do Fim de Vida de uma versão de Serviço Cloud Oracle pode resultar numa actualização automática por parte da Oracle ou numa suspensão dos Serviços Cloud Oracle. Nas situações específicas em que a versão de um Serviço Cloud Oracle atinja o Fim de Vida e a Oracle não disponibilize uma versão actualizada, a Oracle pode indicar e requerer que o Cliente faça a transição para um Serviço Cloud Oracle sucessor.

5 POLÍTICA DE SUPORTE CLOUD ORACLE

O suporte descrito na presente *Política de Suporte Cloud Oracle* aplica-se apenas a Serviços Cloud Oracle e é fornecido pela Oracle como parte desses Serviços Cloud Oracle ao abrigo da Nota de Encomenda do Cliente. A Oracle pode disponibilizar e o Cliente pode encomendar, mediante o pagamento de valores adicionais, ofertas de serviços de suporte adicionais disponibilizadas pela Oracle para os Serviços Cloud Oracle.

5.1 Termos do Suporte Cloud Oracle

5.1.1 Valores de Suporte

Os valores pagos pelo Cliente pelos Serviços Cloud Oracle ao abrigo da Nota de Encomenda do Cliente incluem o suporte descrito na presente *Política de Suporte Cloud Oracle*. Aplicam-se valores adicionais a ofertas de serviços de suporte Oracle adicionais adquiridas pelo Cliente.

5.1.2 Período de Suporte

O suporte Cloud Oracle é disponibilizado a partir da data de início dos Serviços Cloud Oracle e acaba após o término ou resolução dos Serviços ("Período de Suporte"). A Oracle não está obrigada a fornecer o suporte descrito na presente Política de Suporte Cloud Oracle depois do término do Período de Suporte.

5.1.3 Contactos Técnicos

Os contactos técnicos do Cliente são as únicas ligações entre o Cliente e a Oracle relativas a suporte Oracle para Serviços Cloud Oracle. Esses contactos técnicos têm de ter, no mínimo, formação básica relativa ao Serviço e, se necessário, formação complementar adequada para a função ou fase de

implementação específicas, utilização especializada do produto/Serviço e migração. Os contactos técnicos do Cliente têm de estar informados sobre os Serviços Cloud Oracle para ajudarem a resolver problemas do sistema e auxiliarem a Oracle na análise e resolução de Requisições de Serviços. Quando o Cliente apresenta uma Requisição de Serviços, o respectivo contacto técnico deve ter um entendimento básico do problema encontrado e a capacidade para reproduzir o problema, de forma a auxiliar a Oracle no diagnóstico e na triagem do mesmo. Para evitar interrupções no suporte Oracle para Serviços Cloud Oracle, o Cliente tem de notificar a Oracle sempre que as responsabilidades do contacto técnico sejam transferidas para outra pessoa.

5.1.4 Suporte Cloud Oracle

O suporte Oracle para Serviços Cloud Oracle consiste no seguinte:

- Diagnósticos de questões ou problemas relacionados com os Serviços Cloud Oracle
- Esforços comerciais razoáveis para resolver erros comunicados e verificáveis nos Serviços Cloud Oracle para que o respectivo desempenho, em todos os aspectos materiais, corresponda ao descrito na respectiva Documentação do Programa
- Suporte durante actividades de Gestão de Alterações descritas na *Política de Gestão de Alterações Cloud Oracle*
- Assistência com Requisições de Serviços técnicos 24 horas por dia, 7 dias por semana
- Acesso durante 24 horas por dia, 7 dias por semana, a um Portal de Suporte a Clientes Cloud designado pela Oracle (por exemplo, My Oracle Support) e Suporte por Telefone em Tempo Real para registar Requisições de Serviços
- Acesso a fóruns da comunidade
- Assistência de serviços não-técnicos ao Cliente durante o horário normal de expediente da Oracle (das 8:00 às 17:00), hora local

5.2 Sistemas de Suporte a Clientes Cloud Oracle

5.2.1 Portal de Suporte a Clientes Oracle Cloud

A Oracle fornece suporte para o Serviço Cloud Oracle adquirido pelo Cliente através do Portal de Suporte a Clientes Cloud concebido para esse Serviço Cloud Oracle. O acesso ao Portal de Suporte a Clientes Cloud aplicável é regido pelos Termos de Utilização publicados no Web site de suporte designado, estando estes sujeitos a alterações. O acesso ao Portal de Suporte a Clientes Cloud está limitado aos contactos técnicos designados pelo Cliente e a outros utilizadores autorizados dos Serviços Cloud Oracle. Quando aplicável, o Portal de Suporte a Clientes Cloud fornece detalhes de suporte aos contactos técnicos designados pelo Cliente de modo a permitir a utilização do Suporte Oracle para Serviços Cloud Oracle. Todas as notificações e alertas relevantes para o Serviço Cloud Oracle do Cliente são publicados neste portal.

5.2.2 Suporte por Telefone em Tempo Real

Os contactos técnicos do Cliente podem aceder a Suporte por Telefone em Tempo Real através dos números de telefone e das informações de contacto presentes no Web site de suporte Oracle, em <https://www.oracle.com/support/contact.html>.

5.3 Definições de Severidade

Os contactos técnicos do Cliente podem submeter Requisições de Serviços relacionadas com Serviços Cloud Oracle através do Portal de Suporte a Clientes Cloud indicado acima. O nível de severidade de uma Requisição de Serviços apresentada pelo Cliente é seleccionado por este e pela Oracle e tem de se basear nas seguintes definições de severidade:

5.3.1 Severidade 1

A utilização de produção que o Cliente faz dos Serviços Cloud Oracle é interrompida ou o impacto é tão grave que não é possível continuar a trabalhar de modo razoável. A perda de serviço é total. O funcionamento é essencial para o negócio e trata-se de uma situação de emergência. Uma Requisição de Serviços de Severidade 1 tem uma ou mais das seguintes características:

- Dados danificados;
- Uma função crítica documentada não está disponível;
- O Serviço fica bloqueado indefinidamente, provocando demoras inaceitáveis ou indefinidas para recursos ou respostas;
- O Serviço falha repetidamente após tentativas de reinício;
- Incidente de Segurança com o potencial de afectar a confidencialidade, integridade e disponibilidade do Serviço.

A Oracle envidará os esforços razoáveis para responder às Requisições de Serviços de Severidade 1 no espaço de quinze (15) minutos. A Oracle trabalhará 24 horas por dia, 7 dias por semana, até que a Requisição de Serviços de Severidade 1 esteja resolvida, seja implementada uma solução alternativa ou seja possível obter progressos. O Cliente tem de disponibilizar à Oracle um contacto técnico durante esse período de 24 horas por dia, 7 dias por semana, para auxiliar na recolha de dados, nos testes e na aplicação de correcções. O Cliente deverá ser muito cuidadoso ao determinar o grau de severidade, para que as situações válidas de Severidade 1 possam receber a atenção necessária por parte da Oracle.

5.3.2 Severidade 2

A perda de serviço é significativa. Não estão disponíveis funcionalidades importantes dos Serviços Cloud Oracle sem que haja qualquer solução alternativa aceitável; no entanto, as operações podem continuar de forma limitada.

5.3.3 Severidade 3

A perda de serviço é pequena. O problema gera inconvenientes que podem exigir uma solução alternativa para restaurar a funcionalidade.

5.3.4 Severidade 4

O Cliente solicita informações, melhoramentos ou esclarecimentos relativos a documentação dos Serviços Cloud Oracle, mas o funcionamento desse Serviço não é afectado. Não há perda de serviço.

5.4 Alteração do Nível de Severidade de Requisições de Serviços

5.4.1 Nível de Severidade Inicial

No momento em que a Oracle aceita uma Requisição de Serviços, a Oracle regista um nível de severidade inicial da Requisição de Serviços com base nas definições de severidade acima apresentadas. Após aceitação de uma Requisição de Serviços, o enfoque inicial da Oracle estará direccionado para a resolução dos problemas subjacentes à mesma. O nível de severidade de uma Requisição de Serviços pode ser ajustado conforme se descreve abaixo.

5.4.2 Redução do Nível de Requisições de Serviços

Se, durante o processo de Requisição de Serviços, o problema deixar de exigir o nível de severidade actualmente atribuído com base no respectivo impacto actual sobre o funcionamento de produção do Serviço Cloud Oracle aplicável, o nível de severidade será reduzido para o nível de severidade que melhor reflecta o respectivo impacto actual.

5.4.3 Aumento do Nível de Requisições de Serviços

Se, durante o processo de Requisição de Serviços, o problema exigir a atribuição de um nível de severidade superior ao que está atribuído actualmente com base no respectivo impacto actual sobre o funcionamento de produção do Serviço Cloud Oracle aplicável, o nível de severidade será aumentado para o nível de severidade que melhor reflecta o respectivo impacto actual.

5.4.4 Conformidade com as Definições de Nível de Severidade

O Cliente assegurar-se-á de que a atribuição e o ajuste de qualquer designação de nível de severidade são rigorosos com base no impacto actual sobre a operação de produção do Serviço Cloud Oracle aplicável. O Cliente confirma que a Oracle não é responsável por qualquer falha no cumprimento dos standards de desempenho provocada por utilização incorrecta ou atribuição incorrecta de designações do nível de severidade por parte do Cliente.

5.5 Escalonamento de Requisições de Serviços

Em caso de Requisições de Serviços escalonadas, o analista de suporte Oracle envolverá o gestor de escalonamento de Requisições de Serviços da Oracle, que ficará responsável pela gestão do escalonamento. O gestor de escalonamento de Requisições de Serviços da Oracle trabalhará com o Cliente no sentido de desenvolver um plano de acção e atribuir os recursos apropriados da Oracle. Se o problema subjacente à Requisição de Serviços permanecer sem resolução, o Cliente pode contactar o gestor de escalonamento de Requisições de Serviços da Oracle para analisar a Requisição de Serviços e solicitar que esta seja escalonada para o nível seguinte dentro da Oracle, conforme necessário. Para facilitar a resolução de uma Requisição de Serviços escalonada, solicita-se ao Cliente que forneça contactos da sua organização que se encontrem ao mesmo nível do que o atribuído na Oracle relativamente à Requisição de Serviços escalonada.

6 POLÍTICA DE RESOLUÇÃO E SUSPENSÃO CLOUD ORACLE

6.1 Resolução de Serviços Cloud Oracle

Durante um período de sessenta (60) dias após a resolução dos Serviços Cloud Oracle, a Oracle disponibilizará, através de protocolos seguros num formato estruturado e legível electronicamente, os Conteúdos do Cliente existentes nos Serviços Cloud Oracle de produção ou manterá os serviços acessíveis para efeitos de recolha de dados por parte do Cliente.

Para utilizações experimentais gratuitas dos Serviços Cloud Oracle, a Oracle disponibilizará os Conteúdos do Cliente durante um período de trinta (30) dias após a resolução da utilização experimental. Durante este período de recolha, o Acordo de Nível de Serviço Cloud Oracle não é aplicável e o sistema de serviço não pode ser utilizado para quaisquer actividades de produção. A Oracle não tem qualquer obrigação de conservar os Conteúdos do Cliente após este período de recolha.

Se o Cliente necessitar de assistência da Oracle para obter acesso ou cópias dos Conteúdos do Cliente, o Cliente tem de criar uma Requisição de Serviços no Portal de Suporte a Clientes Cloud aplicável ao Serviço (por exemplo: My Oracle Support).

A recolha de dados ou qualquer assistência relacionada por parte da Oracle não se aplica a Serviços Cloud Oracle que não armazenam Conteúdos do Cliente. O Cliente é responsável por assegurar que, se esses Serviços Cloud Oracle dependerem de outros Serviços Cloud Oracle (como o Serviço Cloud Storage ou os Serviços Cloud Database), para o armazenamento de dados, esses outros Serviços Cloud Oracle têm de ter uma duração válida até ao fim da resolução do Serviço Cloud Oracle, para permitir a recolha de dados ou para de outra forma tomar as medidas necessárias para fazer cópias de segurança ou de outra forma armazenar separadamente os Conteúdos do Cliente enquanto a produção de Serviços Cloud Oracle ainda estiver activa antes da resolução.

Após o final do período de recolha, a Oracle eliminará os Conteúdos do Cliente nos Serviços Cloud Oracle (a menos que haja outra obrigatoriedade de acordo com a legislação aplicável).

Para Serviços Oracle Cloud at Customer, o Cliente tem de disponibilizar, para recolha pela Oracle, quaisquer componentes de hardware relacionados com Serviços Oracle Cloud at Customer (incluindo equipamento de gateway) fornecidos pela Oracle em bom estado de funcionamento e nas mesmas condições que no início dos Serviços Oracle Cloud at Customer, sujeitos a desgaste razoável relacionado com uma utilização adequada.

6.2 Resolução de Serviços de Testes Piloto

A presente *Política de Resolução e Suspensão Cloud Oracle* aplica-se a pilotos de produção de Serviços Cloud Oracle. Os pilotos de produção não se encontram disponíveis para todos os Serviços Cloud Oracle.

7 UTILIZAÇÃO DOS SERVIÇOS

Os Serviços Cloud Oracle não podem ser entregues nem ser concedido o respectivo acesso a utilizadores na Venezuela, e os Serviços ou quaisquer resultados dos Serviços não podem ser utilizados em benefício de quaisquer indivíduos ou entidades na Venezuela, incluindo mas não se limitando ao Governo da Venezuela.